

Telefin S.p.A. e il VOIP

Vogliamo iniziare il nuovo anno porgendo a tutti l'augurio per un felice e fortunato 2010. L'anno appena trascorso è stato per Telefin ricco di successi e di progetti prestigiosi e significativi, caratterizzato soprattutto dalla ricorrenza del nostro ventesimo anno di attività.

Lo abbiamo voluto festeggiare il 28 di novembre con i dipendenti ed i collaboratori di Telefin, di Delta Sistemi e di Spe, con le loro famiglie e con tutti coloro che dall'esterno supportano l'impegnativo lavoro della nostra azienda.



e grande per poter ospitare le oltre duecento persone invitate e la scelta è ricaduta su Palazzo di Giardino Giusti, una cornice meravigliosa nel cuore della nostra bellissima Verona. Quando la festa volgeva ormai al termine e le persone cominciavano a lasciare le sale di questo splendido palazzo, più di qualche operatore che aveva curato i particolari dell'evento ci ha confermato che nel corso dei lunghi anni della propria esperienza, poche volte si era ritrovato coinvolto in un evento aziendale dal sapore così familiare.

Sono passati ormai vent'anni, sono passati solo vent'anni, trascorsi molto velocemente, passati benissimo ed il merito è di tutti coloro che hanno portato, chi fin dall'inizio, chi in corsa, il proprio lavoro, la professionalità, l'esperienza e soprattutto la passione.

Non a caso "telecomunicare con passione" è lo slogan di Telefin, a sottolineare che la chiave del successo di un'azienda non sono solo freddi calcoli finanziari, ma la creazione di un clima di rispetto, di armonia e di collettività. Tutti questi elementi sono la marcia in più di questa nostra azienda, quegli elementi che ci hanno permesso anche di attraversare e superare momenti difficili ed arrivare fino a qui. In un periodo di cosiddetta crisi infatti, vediamo molte aziende in difficoltà anche nel nostro settore, Telefin invece continua non solo a mantenere i livelli occupazionali, ma addirittura a crescere; guardando sempre al futuro, sfornando idee, progetti e sistemi per l'infrastruttura ferroviaria tra i più moderni ed evoluti.

L'augurio è che si continui così, che assieme alla professionalità, allo zelo ed all'inventiva non si perda mai il sorriso e la voglia di portare alla società qualcosa di sempre più perfezionato, di sempre più evoluto a beneficio del cliente e del Paese tutto.

Bertucci, Cabaletti,
Fogliani, Peroni

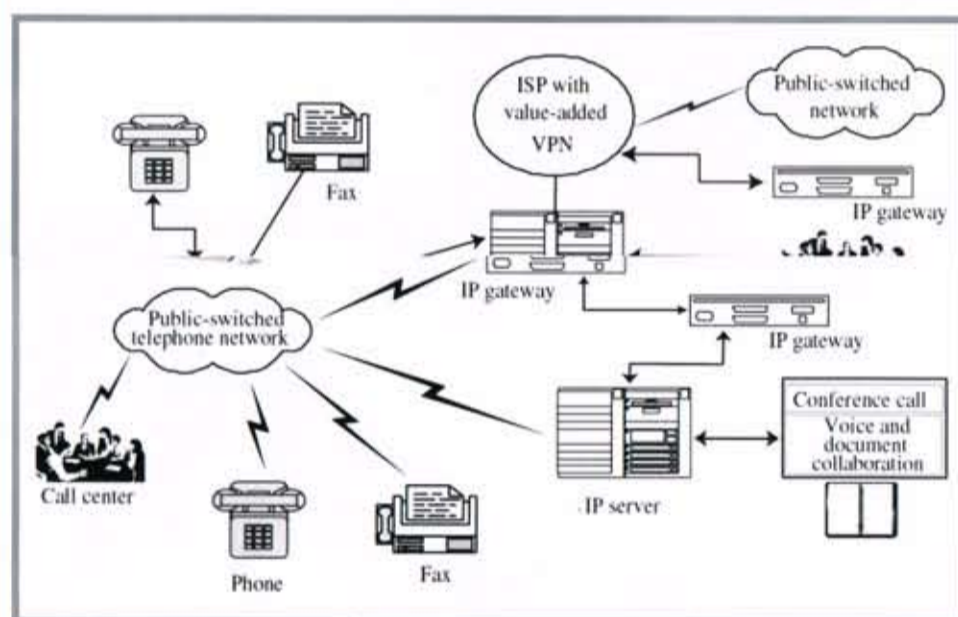
Telefin S.p.A. si è affermata anche per l'attenzione e l'interesse per le innovazioni tecnologiche, e non poteva certo non approfondire la tematica del VOIP, farla propria e applicarla al campo dell'impiantistica ferroviaria. Fino a giungere alla realizzazione, in questi due ultimi anni, degli impianti STI di Palermo, i due di Bologna AV e Is e il recentissimo Settimo Torinese che insiste anch'esso sulla linea AV. Come è noto, tali impianti sono molto complessi e nascono proprio dalla filosofia e architettura TCP/IP. Negli stessi impianti realizziamo la completa commutazione e interfacciamento di tutti i servizi e circuiti esistenti in Ferrovia verso la tecnica VOIP. Le nostre consolidate collabo-

razioni con la Facoltà di Telecomunicazioni dell'Università degli Studi di Trento e con il Dipartimento di Informatica dell'Università degli Studi di Verona ci consentono un aggiornamento continuo sulle nuove ricerche e sviluppi tecnologici. La nostra più che ventennale conoscenza del ferroviario ci permette, successivamente, di sviluppare soluzioni e applicazioni tarate sul ferroviario.

Già nel primo numero di questo giornale aziendale (febb. 2008) dedicammo una pagina all'argomento "progettazione e simulazione di una rete per servizi vocali in ambito ferroviario". Fu il risultato di una brillante tesi di ricerca

e sperimentazione condotta presso i nostri laboratori. Venivano simulate due diverse situazioni: la galleria del Frejus e la tratta ferroviaria Alessandria-Torino.

Due scenari diversi, il primo caratterizzato da una grande mole di dati veicolati dal sistema di emergenza in galleria, e l'altro meno pesante ma altresì legato alla regolarità dell'esercizio ferroviario. Da ognuna di tali simulazioni abbiamo tratto importanti indicazioni per una corretta progettazione, rilevando che da una non attenta selezione di protocolli e codifiche potrebbero, in talune situazioni, sorgere inconvenienti (anno 1, n° 1 febr. 2008).



VOIP Security

Negli ultimi anni, con la proliferazione delle reti IP, emerge la tecnologia VOIP come alternativa alla tradizionale rete telefonica, offrendo l'opportunità di utilizzare una singola rete a commutazione di pacchetto, anziché più reti dedicate e separate, per il trasporto di dati, voce e video.

L'architettura VOIP spinge l'intelligenza del sistema dalle centrali verso i dispositivi terminali (PCs, IP phone, ecc.), con la possibilità di creare molti nuovi servizi che non potevano esistere sulle reti di telefonia tradizionale, oltre che supportare quelli già esistenti. In futuro, i servizi VOIP dovranno operare in modo trasparente su un'unica rete convergente, costituita dalla combinazione di reti eterogenee che comprendono

VOIP

Lo scorso 10
Dicembre, il nostro



Riccardo Venturini ha conseguito la Laurea di primo livello in Informatica presso il Dipartimento di Informatica dell'Università degli Studi di Verona. Il dott. Venturini ha sviluppato una tesi su Sicurezza nel VOIP, della quale riportiamo di seguito una sintesi di alcuni articoli. Tale lavoro si inserisce a pieno titolo nel processo di ricerca e sviluppo in corso nella nostra Azienda.

Riccardo Venturini (Telefin S.p.A.)

reti packet-switched, circuit-switched e wireless. In pratica, però, i vantaggi provenienti dall'uso di una rete dati anche per la voce sono mitigati, oltre che dai normali problemi di sicurezza già conosciuti per le reti IP, che possono attaccare il VOIP sia nella segnalazione che nei dati, dalla nascita di nuove problematiche, come la qualità del servizio e la sicurezza della comunicazione.

Luci ed ombre del VOIP

Nelle attuali reti a commutazione di circuito (PSTN) le minacce alla sicurezza sono considerate pressoché minime, perché tali reti sono, in un certo senso, chiuse. Ma in un ambiente aperto, come le reti WAN o Internet, progettare un attacco ad un server di telefonia VOIP è molto più semplice ed economico: basta avere una connessione alla rete. Sia la segnalazione che i dati sono nuove possibili vittime di attacchi già noti in ambito Internet, gli utenti che comunicano tramite VOIP sono, quindi, tutti potenziali vittime di ascolto della conversazione. La telefonia IP utilizza l'architettura Internet similmente alle normali applicazioni.

Ciò nonostante, in particolare dal punto di vista della sicurezza, il VOIP è differente per tre principali ragioni:

- Necessita di considerazioni particolari per la configurazione dei dispositivi di rete (es. firewall)
- Natura real-time: un pacchetto che arriva tardi è inutile
- Separazione dei dati dal segnalamento. Le sessioni, in particolare quelle nuove in ingresso, che definiscono informazioni di indirizzamento del canale multi mediale non funzionano bene in presenza di NAT (Network Address Translation) e cifratura.

Nel campo informatico, la sicurezza consiste nel prevenire e individuare azioni improprie al sistema. I servizi fondamentali da garantire sono:

- **Confidenzialità:** prevenire l'apprendimento dell'informazione, che può avvenire anche senza l'accesso diretto ai dati. Implica l'autenticazione delle parti (e dei dati).
- **Autenticazione:** verifica dell'identità
- **Integrità:** prevenire modifiche non autorizzate
- **Disponibilità:** garantire la qualità del servizio

segue a pagina 2 >

I principali attacchi a cui è soggetto il VOIP possono essere suddivisi nelle seguenti categorie:

• Denial Of Service (DoS)

Oltre al problema delle intercettazioni, il VOIP è soggetto soprattutto ai fenomeni tipici delle reti a commutazione di pacchetto, quali jitter e perdita di pacchetti. Jitter è il fenomeno generato dal ritardo con cui giungono a destinazione i pacchetti che trasportano la voce. Per poter ricostruire lo stream multimediale, il VOIP, contrariamente a quanto vale per gli altri tipi di connessione su IP, richiede che i pacchetti contenenti i frame audio arrivino non solo in modo veloce e fluido, ma anche il più possibile nello stesso ordine con cui sono partiti. Nella ricostruzione della voce, infatti, è intuitivo capire che questo è un parametro importante, contrariamente a quanto può esserlo nella ricostruzione di una pagina web. La congestione della rete, percorsi diversi tra i vari pacchetti, larghezza di banda insufficiente, sono tutte cause che determinano il degrado della voce trasportata su rete IP e in particolare causano il ritardo, anche di vari millisecondi, tra un pacchetto e l'altro. Una perdita pari o superiore al 10% non consente di svolgere una chiara comunicazione. Le attuali reti IP non dispongono di meccanismi in grado di garantire che i pacchetti vengano ricevuti nello stesso ordine con cui sono stati trasmessi, né che non ci siano perdite di pacchetti.

In figura 1 un esempio di ritardo dovuto alla rete di interconnessione.

Per garantire la qualità della conversazione nel VOIP, quindi, sono necessari:

- coerenza temporale dello stream audio
- tempo di latenza sufficientemente basso (vedi figura 2)

Un attacco mirato alla diminuzione della banda disponibile, quindi, può facilmente portare ad avere ritardi e perdite di parti della voce trasmessa e quindi ad una comunicazione non accettabile. Tuttavia, tali attacchi possono essere mirati anche all'aumento del packet-rate, che aumenta il carico di lavoro dei server pur mantenendo bassa la banda utilizzata. In generale, il packet-rate di un attacco può avere un impatto maggiore di un attacco alla banda. In questi casi, è possibile agire contro attacchi al protocollo, ma risulta di difficile individuazione un attacco mirato al sovraccarico del sistema, perché si dovranno distinguere gli accessi legittimi da quelli non legittimi. L'utilizzo di meccanismi per la sicurezza (es. cifratura, autenticazione, filtraggio), aumenta ulteriormente il carico di lavoro e i tempi di latenza, si deve quindi impiegare un'architettura di sistema adeguata ed efficiente.

La cifratura può operare su diversi layer TCP/IP: (vedi figura 3 e 3a)

	OSI	TCP/IP	Encryption
7	Applicazione	Applicazione	End-to-End
6	Presentazione		
5	Sessione		
4	Trasporto	TCP	Link
3	Network		
2	Data link		
1	Fisico		

Figura 3

Garantire una larghezza di banda sufficientemente ampia, quindi, è relativamente semplice nelle piccole reti (es. LAN), ma è molto più difficile nelle vaste reti eterogenee come le reti Internet.

• Eavesdropping: intercettazione e modifica

Un hacker non sempre ha bisogno di inserirsi tra due utenti per intercettare o modificare la comunicazione: può farlo anche inviando richieste a server proxy non sicuri o mal configurati per ridirigere le chiamate in ingresso e uscita. L'intercettazione del flusso di segnalamento permette di ottenere dati sensibili, che possono anche essere riutilizzati per attivare ulteriori attacchi, come man-in-the-middle, uso di falsa identità e replay. L'intercettazione del flusso dei dati permette di ascoltare le conversazioni o addirittura tradurle in testo scritto. Inoltre, l'omissione o alterazione dello stream multimediale può cambiare drasticamente il significato di una conversazione. (vedi figura 4)

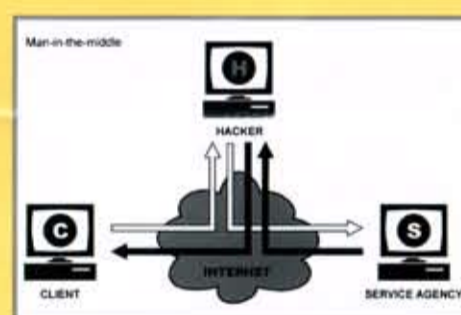


Figura 4

• Packet injection: iniezione di pacchetti

Invio di vecchi pacchetti VOIP agli utenti in conversazione, inserendo voce, disturbi o vuoti. Per esempio, se in una conferenza viene usato RTP senza autenticazione, si può aumentare il numero di utenti iniettando pacchetti con id sorgente diverso, portando così al sovraccarico del sistema. Altro tipo di attacco al protocollo RTP, che può portare al degrado della conversazione, è l'invio di pacchetti contenenti numeri casuali sia nell'header che nel payload.

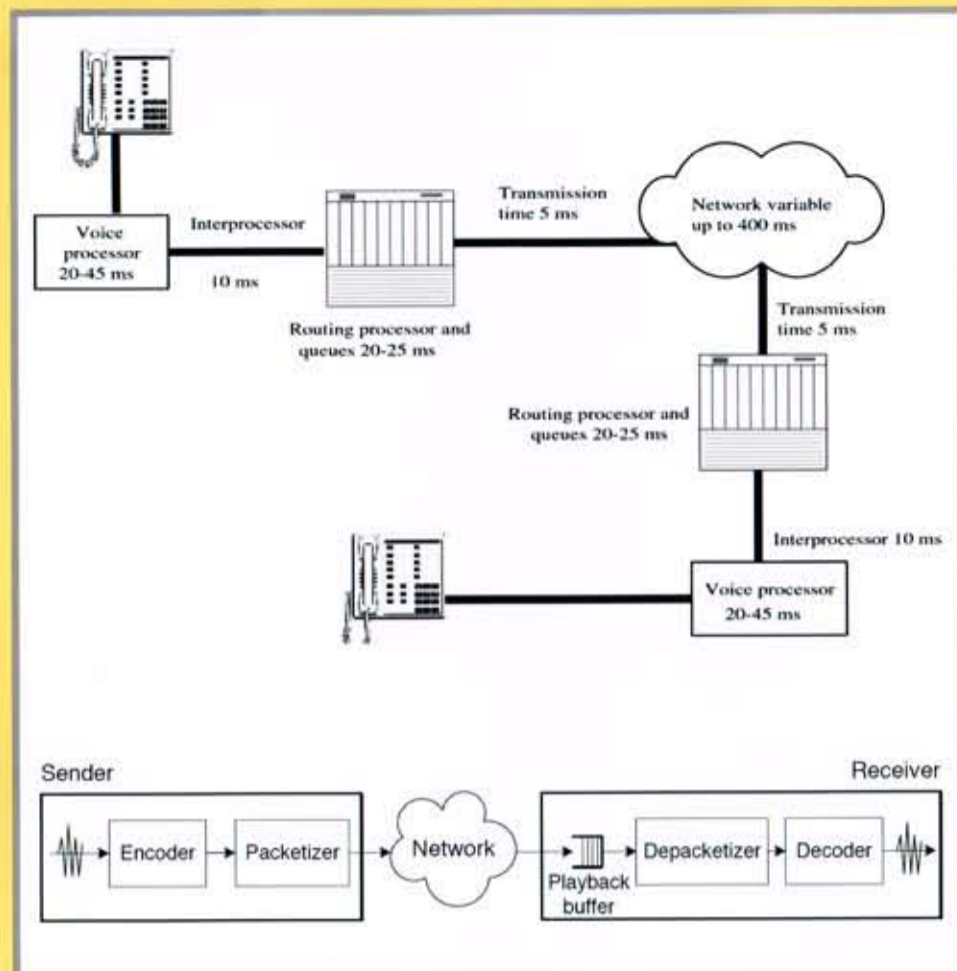


Figura 1 - esempio di ritardo

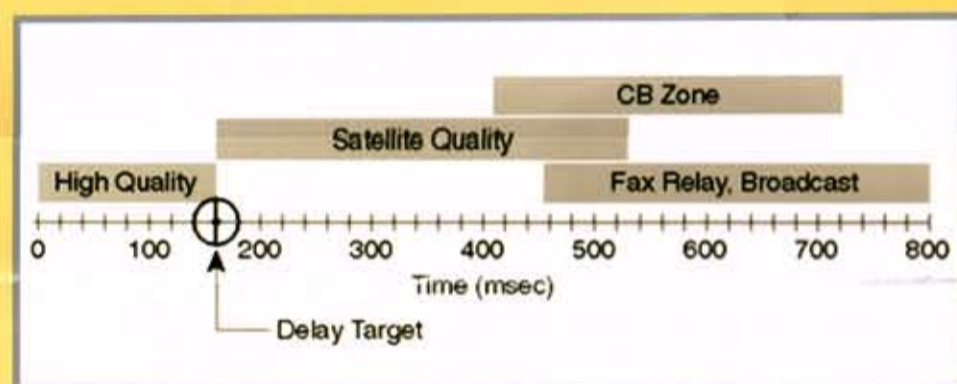


Figura 2

	Link Encryption	End-to-End Encryption
Autenticazione	Host	Utente
Dove	Ad ogni link (es. gateway)	Tra host sorgente e destinazione
Distribuzione chiavi	Una coppia di chiavi per ogni coppia di device sulla rete (nodi intermedi)	Una sola coppia di chiavi tra mittente e destinatario
Cifratura	Header IP cifrato, con sostituzione dell'indirizzo IP: contenuto e flusso protetto	Header IP in chiaro: contenuto protetto, flusso del traffico no
Esposizione	Messaggio esposto nei nodi intermedi e negli host	Messaggio protetto nei nodi e negli host
Implementazione	Hardware o software	Software
Gestione	Trasparente all'utente	L'utente seleziona la cifratura
Flessibilità	Tutti i messaggi o nessuno	Selettivo

Figura 3a

Attacchi e possibili soluzioni

La seguente tabella mostra alcuni attacchi per categoria, il servizio attaccato e una possibile soluzione generale: (tabella a)

Attacco	Servizio attaccato Aut. Int. Conf. Disp.	Possibile soluzione
Eavesdropping	Tracciamento dei pattern di chiamata	Cifratura della segnalazione
	Cattura del traffico	Cifratura della segnalazione e dei dati
	Raccolta degli ID	Cifratura della segnalazione
	Ricostruzione dei dati	Cifratura dei dati
Intercettazione e modifica	Insabbiamento di chiamata	Protezione della segnalazione
	Dirottamento di chiamata	Protezione della segnalazione
	Alterazione dei dati	Protezione dei dati
	Degrado della conversazione	Protezione della segnalazione e dei dati
	Uso di falsa identità	Autenticazione dell'utente e della segnalazione
DoS	Contatti indesiderati	Autenticazione dell'utente
	Flooding di richieste	Monitoraggio e filtraggio del traffico
	Messaggi malformati	Parser di messaggi (IDS)
	Attacco al servizio	Protezione della segnalazione
VoIP Specific	Messaggi fittizi	Protezione della segnalazione
	Dirottamento di chiamata	Protezione della segnalazione
DoS Generale	Esaurimento delle risorse	Monitoraggio e filtraggio del traffico
	Al meccanismo di autenticazione	Architettura del server più efficiente
	Al'architettura sottostante	Architettura del server più efficiente

Layer	Attacco	Aut./Conf.	Integrità	Disponib.
Network	Physical	X	X	X
	ARP cache	X	X	X
	ARP flood	X	X	X
	MAC spoofing	X	X	X
Internet	Redirect via IP spoofing	X	X	X
	Device	X	X	X
	Malformed packets	X	X	X
	IP frag	X	X	X
Transport	Jolt	X	X	X
	TCP/UDP flood	X	X	X
	TCP/UDP replay	X	X	X
	TFTP server insertion	X	X	X
Application	DHCP server insertion	X	X	X
	DHCP starvation	X	X	X
	ICMP flood	X	X	X
	Registration Hijacking	X	X	X
	Message modification	X	X	X
	RTP insertion	X	X	X
	Spoof via header	X	X	X
	Malformed method	X	X	X
	Redirect method	X	X	X
	RTP payload	X	X	X
	Default configuration	X	X	X
	Unnecessary services	X	X	X
	Buffer overflow	X	X	X
	DNS Availability	X	X	X

Posizionamento su layer TCP/IP (tabella b)

TT596 e Telefonia Selettiva VOIP:

Un nuovo obiettivo per Telefin S.p.A.

Nel mese di giugno 2009 è stata emessa da parte di RFI la Specifica Tecnica TT596 "Specifiche per la realizzazione di un sistema di telefonia VOIP".

Tale documento pone lo scopo di rinnovare e semplificare gli impianti di telefonia selettiva per i circuiti DC, DU, DCO, MAN e DOTE utilizzando tecnologie innovative di facile manutenibilità. La Specifica richiede l'utilizzo di apparecchiature di tipo commerciale e di semplice reperibilità sul mercato: l'impianto dovrà garantire una particolare flessibilità per una integrazione con le tecnologie esistenti allo scopo di utilizzare Posti di Lavoro e

Telefoni di Linea già presenti nelle tratte interessate al rinnovo (anche parziale) degli impianti di telecomunicazione.

L'architettura generale del nuovo sistema VOIP è caratterizzata da una rete IP come unico supporto trasmissivo per tutti i circuiti di telecomunicazione attualmente presenti nelle linee di tipo C e D della rete ferroviaria nazionale. Il sistema prevede l'utilizzo di modem drop-insert predisposti con interfacce di linea dedicate che possono indifferentemente connettersi ai diversi assi trasmissivi messi a disposizione da RFI (flusso 2Mbit/s,

interfaccia di linea SHDSL o collegamento in fibra ottica). All'interno di ogni stazione sarà sviluppata una rete LAN costituita da Switch Ethernet collegati ad ogni singolo Modem. Agli Switch verranno collegate tutte le apparecchiature necessarie tipiche di una struttura di telecomunicazione VOIP: centrale IP-PBX, IP-Phone, Console Operatore Touch-Screen ad uso del DCO/DOTE, interfacce utenti (ATA) per il collegamento di telefoni stagni BCA di linea o di piazzale esistenti.

Per ridurre al minimo la possibilità di disservizi ogni singolo apparato dovrà essere diagnosticabile e configurabile da remoto tramite un sistema di supervisione centralizzato; il sistema deve inoltre prevedere la possibilità di una richiusura ad anello dell'asse trasmissivo per sopperire ad eventuali interruzioni lungo linea. In tal caso i modem drop-insert presenti in ogni stazione consentiranno di scegliere la via con i tempi di propagazione più bassi, ottimizzando così la comunicazione. L'obiettivo di Telefin sarà quello di coniugare l'esperienza pluriennale nell'ambito della

telefonia selettiva tradizionale e, negli ultimi anni, nel campo della Telefonia VOIP maturata e affermata nella realizzazione degli impianti STI, per soddisfare al meglio le caratteristiche richieste dalla nuova Specifica TT596. Intendiamo apportare funzionalità atte a rendere l'impianto flessibile e idoneo a qualsiasi regime di esercizio delle linee ferroviarie.

Nel rispetto della "Specifiche dei requisiti funzionali per gli impianti di telefonia per l'esercizio ferroviario" (TT595), grazie alla nostra esperienza implementeremo nel nuovo sistema, per quanto possibile, le funzionalità tipiche richieste dall'attuale esercizio ferroviario nei vari regimi di circolazione, quali V°BIS, V°TE, DCO, MAN, DOTE, T luminose, telediffusione sonora (TDS) e ovviamente, laddove presente, la Telefonia GSMR osservando le disposizioni delle specifiche EIRENE MORANE relativamente alle funzionalità di dispatcher.

Diego Nalin (Telefin S.p.A.)

Saremo presenti alla prossima edizione di EXPO Ferroviaria 8 - 10 Giugno 2010, presso Lingotto Fiere, Torino, Italia

Vent'anni di Telefin S.p.A.

Il 28 novembre 2009 Telefin S.p.A. ha festeggiato il ventesimo anno di attività nei meravigliosi locali di Palazzo Giusti a Verona, una splendida residenza del XVI secolo, circondata da un giardino tra i più famosi al mondo. Pur inseriti in un ambiente così prestigioso, la giornata si

è subito caratterizzata per il clima informale e cordiale che si è instaurato tra gli oltre 200 ospiti, collaboratori e dipendenti accompagnati dalle proprie famiglie, come documentato da questa ricca galleria fotografica.



Stazione di VENT'ANNI.

Una stazione ricca di significati e valori per un viaggio importante, che passando per ricerca e sviluppo porta all'innovazione. Un treno carico di esperienza al servizio delle telecomunicazioni ferroviarie. Da vent'anni questo viaggio è il nostro lavoro.

Per conoscere le prossime stazioni: www.telefin.it

Via Albani, 87/A - 37138 Verona - Italia Tel. +39 045 8106404



SITRAM

Localizzazione automatica dei treni e informazione a bordo.

Ferrovie del Nord Barese S.p.A., Metronapoli S.p.A. e Sistemi Territoriali S.p.A. sono solo alcune delle importanti referenze che hanno scelto di affidare a Delta Sistemi s.r.l. il compito di migliorare la qualità del servizio di trasporto ai passeggeri attraverso l'informazione a bordo treno e in stazione. Progetto guida in questi ultimi anni e fonte di notevoli soddisfazioni è SITRAM: il sistema che provvede alla localizzazione automatica del treno in linea abilitando (in ogni istante) a bordo informazioni visive e sonore ai passeggeri.

La capacità di integrare diverse tecnologie e la grande esperienza del suo Ufficio tecnico ha consentito a Delta Sistemi s.r.l. di produrre soluzioni innovative ed esclusive in grado di garantire la piena funzionalità del sistema in qualsiasi situazione (anche in galleria o zone non raggiunte dal segnale GPS). PC di bordo, pannelli informativi, sistemi di rilevamento a Radio Frequenza, sistemi di diffusione sonora sono prodotti e personalizzati da Delta Sistemi s.r.l. in base alle richieste dei clienti.

Oltre all'informazione in tempo reale SITRAM offre la possibilità di integrare un sistema di

videosorveglianza digitale ad alta definizione in grado di contribuire alla riduzione degli atti vandalici attraverso l'effetto deterrente delle telecamere. Le immagini vengono registrate e visualizzate attraverso un sistema WIFI direttamente sui monitor installati a bordo treno, oltre che al centro di controllo. Riassumendo, le principali funzioni di SITRAM sono:

- la localizzazione al centro di supervisione dei mezzi in linea
- informazione audio/video a bordo, informazione audio/video a terra, videosorveglianza
- il controllo degli apparati tecnologici di bordo
- il supporto automatico della manutenzione dei rotabili
- la creazione e gestione di palinsesti di visualizzazione al pubblico.

Enrico Frattini, presidente della Delta Sistemi s.r.l., afferma che: oltre alle indiscusse capacità tecniche, grande merito del successo dei nostri impianti è da attribuire ai nostri clienti che con attenzione, critiche e volontà supportano in ogni momento la crescita e lo sviluppo dei sistemi. Delta Sistemi s.r.l. non presenta mai la stessa soluzione... ogni sistema è tagliato e cucito su misura.

Delta Sistemi s.r.l.

Nuovo marchio e nuova sede per l'azienda



Delta Sistemi

v progetto nuova sede

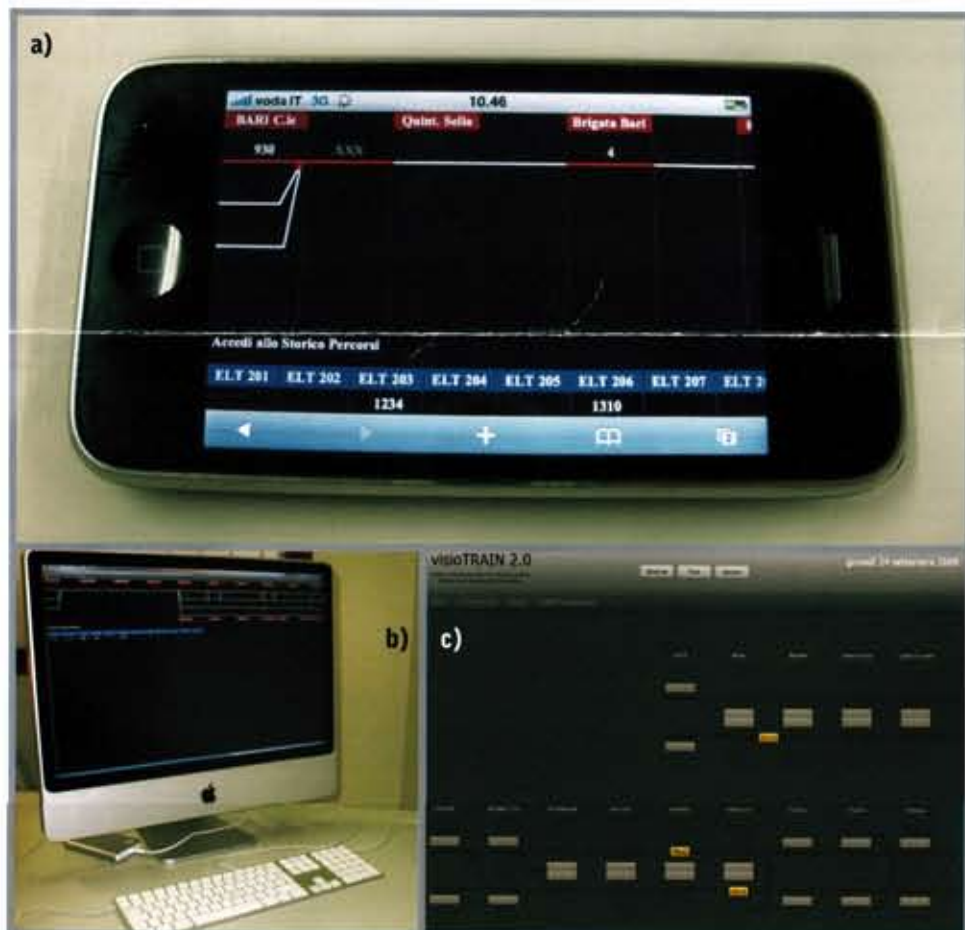


Fondata nel 1995 Delta Sistemi s.r.l. ha sin dall'inizio orientato la sua attività principale verso la progettazione e lo sviluppo di sistemi integrati hardware e software per il trasporto ferroviario e metropolitano.

Delta Sistemi s.r.l. può oggi vantare di essere l'azienda di riferimento nei servizi che essa propone, in un'ottica di costante ricerca di qualità e innovazione. Nel corso degli anni la società ha potenziato le proprie competenze tecniche sviluppando un ampio know-how, diventando interlocutore di riferimento per molte società di trasporto pubblico. In quest'ottica si affaccia al 2010 pronta per un vero e proprio restyling aziendale che ha comportato anzitutto il mutare del suo marchio storico e che nei prossimi mesi si completerà con il trasferimento della sede.



Il Presidente
Enrico Frattini



- a) Visualizzazione treni su smart phone
b) Visualizzazione treni su postazione operatore
c) Dettaglio Visiotrain: visualizzazione treni
d) Monitor installato presso Circumvesuviana S.p.A.
e) Monitor installato presso Metronapoli S.p.A. - Linea 1
f) Monitor installato presso Metronapoli S.p.A. - Funicolare
g) Monitor installato presso Ferrotramviaria S.p.A.
h) Visualizzazione immagini a bordo treno
i) Panoramica: monitor installato presso Ferrotramviaria S.p.A.



TELECOMUNICARE CON PASSIONE